INFORMATION SECURITY
...is good Business

Survival Tools & Techniques

Information Security: Defining Your Needs

Page 1

Content Notes

Presentation Notes

Have slide showing as attendees assemble.

Introduce yourself, giving a brief review of IS background and instructional experience.

NOTE: Be prepared to answer questions throughout the presentation. If attendees look as if they do not understand a given point, take time to explain.

Information Security Solutions

Analysis

People

Technology

Procedures

Analysis: Defining Your Needs

What are you going to protect?

Security Policies

Where are you vulnerable?

Risk Assessment

Page 3

Content Notes

The first step is analysis. These are the 2 questions that have to be considered.

- What are you going to protect?
- Where are you vulnerable?

Presentation Notes

Explain that before jumping ahead to implement Information Security, businesses should plan for the most effective use of their investment. To do so, they need to ask themselves these 2 questions.

Explain that skipping this step means potential loss of investment and ineffectiveness of IS procedures.

Analysis: Defining Your Needs

What are you going to protect?

Security Policies

Where are you vulnerable?

Risk Assessment

Content Notes

The first step is analysis. These are the 2 questions that have to be considered.

- What are you going to protect?
- Where are you vulnerable?

Presentation Notes

Explain that before jumping ahead to implement Information Security, businesses should plan for the most effective use of their investment. To do so, they need to ask themselves these 2 questions.

Explain that skipping this step means potential loss of investment and ineffectiveness of IS procedures.

Security Policies

A Security Policy defines:

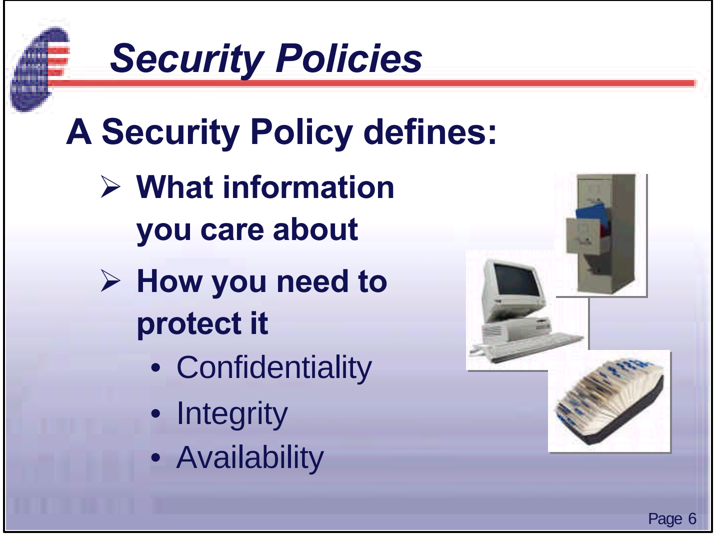
- **What information you care about**
- **How you need to protect it**

Content Notes

Presentation Notes

Ask attendees who work for a company that already has a security policy to raise their hands. Count the hands and give the whole group a rough percentage.
Compliment those who have policies in place and assure the whole group that by the end of the presentation, with their notes and resources, they will have the essentials for producing their own policies.

Explain that a security policy deals with both the "what" and the "how." That is, it deals with what needs to be protected and the type of protection.



Security Policies

A Security Policy defines:

- **What information you care about**
- **How you need to protect it**
  - Confidentiality
  - Integrity
  - Availability

Page 6

Content Notes

Define:

- Confidentiality
- Integrity
- Availability

Presentation Notes

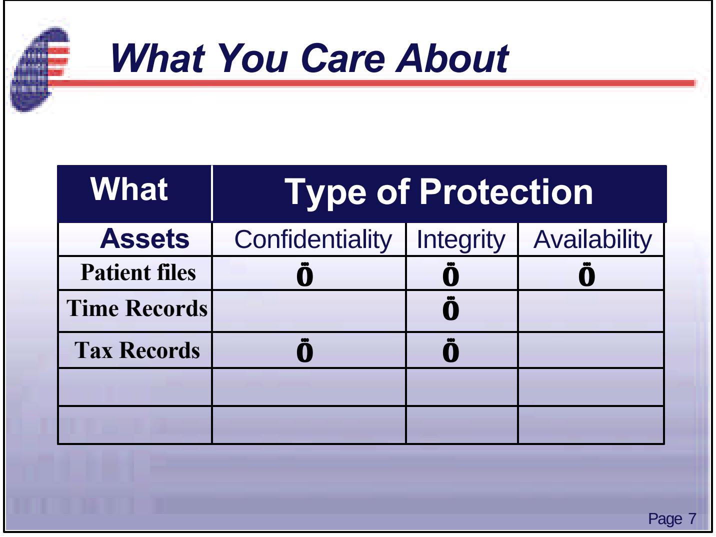
Review: Confidentiality, Integrity, Availability

Explain that as they identify assets, they need to prioritize what aspect of IS is most important to them:
• confidentiality
•integrity
•availability

Ask how many would say confidentiality is the main issue for their company. Ask for a show of hands. Call on 1 person to explain why that attribute is important to their company.

Do the same for integrity and availability.

Give example of an instance when access Vs. control issue arises.



What You Care About

What	Type of Protection		
Assets	Confidentiality	Integrity	Availability
Patient files	ō	ō	ō
Time Records		ō	
Tax Records	ō	ō	

Content Notes

What Information assets are you trying to Protect?

- Data - files, plans, …
- Processes - programs, business applications,
- Hardware - computers
- Facility - rooms, offices
- Mission - private business decisions and strategies

Consider When Defining Assets and Protections:

- What happens if this information falls into someone else’s hands?
- How much would it cost me to be without this information?
- How much would it cost me to re-create this information?
- Which is more important, free access or absolute control?
- Other factors: reputation, integrity

Presentation Notes

Give an example for integrity.

Creating Your Security Policy

- Identify your assets
- Acceptable use policies
- Applicable protection
- Privacy regulations
- Business security rules

Page 8

Content Notes

Start with what security means to your business and its mission.

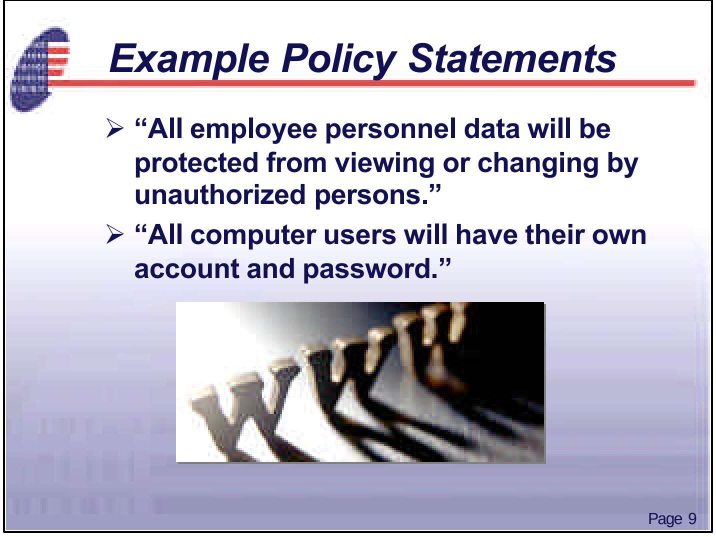
Define an overall code of business behavior.

Determine what company information is private and what is public.

Presentation Notes

Explain that they need to identify assets and consider which of these applies to each.

Ask them to give examples of their assets, including processes handled thru their computers and networks.



Example Policy Statements

- “All employee personnel data will be protected from viewing or changing by unauthorized persons.”
- “All computer users will have their own account and password.”

Content Notes

Large businesses usually develop Security Policies with four basic sections:

- Introduction & References
  - Driving company, industry, or regulatory policies
  - Scope of Policy (is it IT only? Broad operations policy?)
    - Important to list what is not addressed by this policy (and hopefully where it is addressed)
  - Statement on how this policy is maintained and approved
- Definitions
  - List of terms (Confidentiality, Integrity, …) used in the policy
  - Definition of proprietary information
- Assumptions
  - Basic assumptions that may ultimately affect the sufficiency of the policy
    - Policy is for “U.S. only operations”
    - Users have been trained and acknowledge this policy
- Policy Statements

Some Additional Elements to Policies

Statements on Internet Access and Usage

What is acceptable and non-acceptable use of the Internet?

  - What protections must govern email usage?
  - Statements on System Accounts
- How is user access to systems managed?
  - Who approves access?
  - Example: “Each computer user will have their own user id and password”

Analysis: Defining Your Needs

Security Policies

Risk Assessment

Page 10

Content Notes

Once you’ve got a good idea of what security is to your business, and what it is you’re trying to protect, then you can decide what you need to do about it.

This process is called **“Risk Assessment”** and it is critical to meeting all of the security and business goals we discussed before.

Presentation Notes

Ask what the usual definition is for “risk assessment.” **Explain** how the term is used in IS.

Security Risk Assessment

Identify:

- Threats
- Vulnerabilities
- Risks

Content Notes

Security Risk Assessment is deciding what needs attention in order to secure your information.

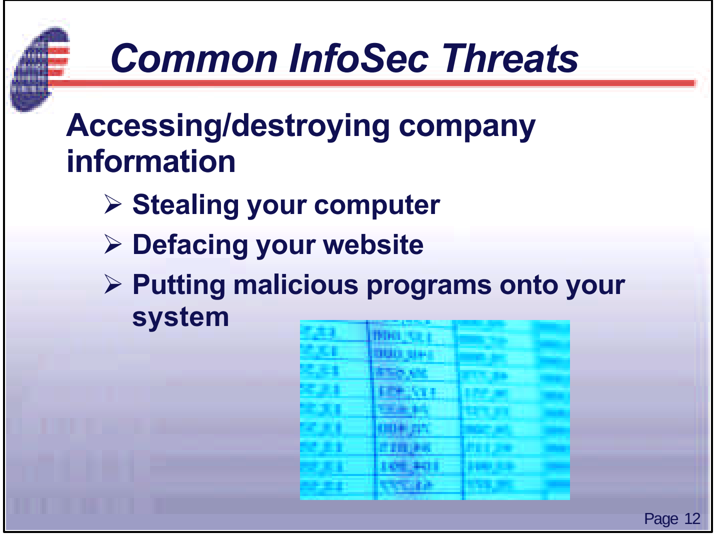
Need to identify:

- **Threats** to the security of your assets (What can happen?)
- **Vulnerabilities** that you have to these threats (How can it happen?)
- **Risks** that you have from threats exploiting these vulnerabilities
  - Consider the likelihood and the consequences in evaluating risk

Presentation Notes

Ask for ideas on “what needs attention.”

Give an example:
For one asset, go through each question -
What could happen?
How could it happen?
What risk does that threat pose?



Common InfoSec Threats

Accessing/destroying company information

- ➢ Stealing your computer
- ➢ Defacing your website
- ➢ Putting malicious programs onto your system

Content Notes

Someone getting into your computer in the office and accessing/destroying/changing company information
Walking up to the computer (no password)
Finding, guessing, or stealing password

How likely is it that someone will try to do these?
Probably high, given human nature and the ease at which these can be tried

All threats originate from humans or nature

Some Common Information Security Threats:

- Someone getting into your computer in the office and accessing/destroying company information
- Someone stealing your computer
- Someone defacing your web site
- Someone putting malicious programs onto your system

Presentation Notes

Briefly explain how this could happen.

Ask for an example “from nature.”

Threats (continued)

Other Threats

- **Spoofing**
- **Snooping**
- **Social engineering**
- **Abuse of system privileges**

Page 13

Content Notes

Other Threats (technical and non-technical)

- Spoofing: Someone or thing pretending to be someone else
- Snooping: wiretaps or network data capture
- Social Engineering
  - Dumpster diving
  - Inquisitive people, “Sales calls”
  - “Help Desk” calls
- Your administrators abusing system privileges

Presentation Notes

Ask (if there is time) for ideas as to what these mean
Explain each.

Ask for examples of threats to their own assets.

Security Risk Assessment

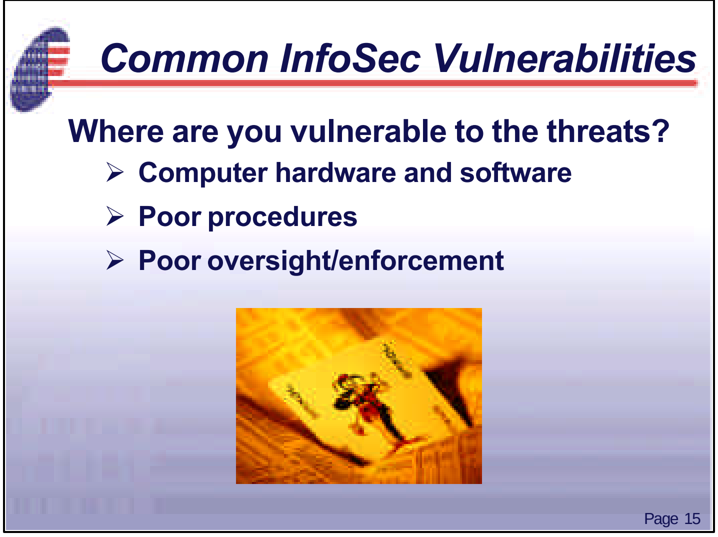
Identify:

- Threats
- **Vulnerabilities**
- Risks

Content Notes

Identify **vulnerabilities** (How can it happen?) that you have to these threats.

Presentation Notes



Common InfoSec Vulnerabilities

Where are you vulnerable to the threats?

- Computer hardware and software
- Poor procedures
- Poor oversight/enforcement

Page 15

Content Notes

Consider where you can be vulnerable to the threats:

- Your people's behavior
- Your business procedures
- Computer hardware (bugs)
- Operating systems (Login, file systems)
- Computer software (office Productivity tools, Utilities)
- Network and Internet connections
- Web Services
- Databases
- Specialized applications (Accounting, Inventory Control,…)
  - Especially applications you develop in-house

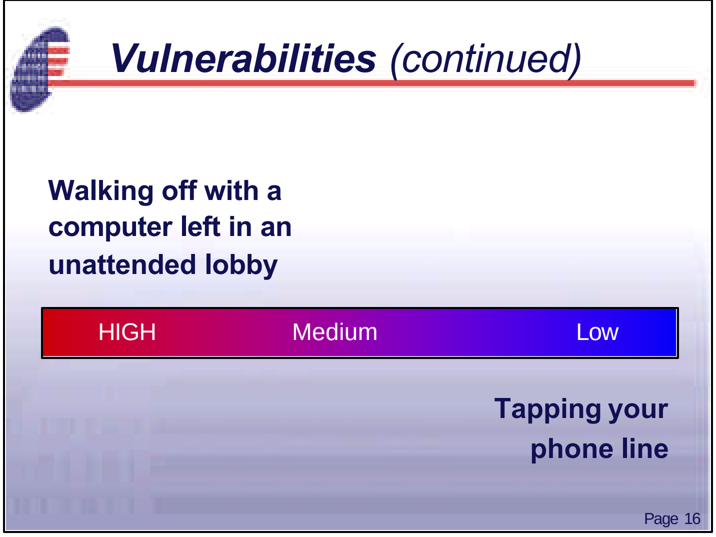
Consider consequences of poor management and poor procedure

- Allowing accounts with none, default, or weak passwords
- Open file sharing
- Direct modem or Internet connections with no safeguards
- Allowing executables to run with full privileges
- Allowing people to have full privileges

Presentation Notes

Ask for a few examples from their experiences: software bugs/ business procedure, etc.

Explain briefly what an executable is. **Ask** how many attendees have already had trouble with these.



Vulnerabilities *(continued)*

Walking off with a computer left in an unattended lobby

HIGH	Medium	Low

Tapping your phone line

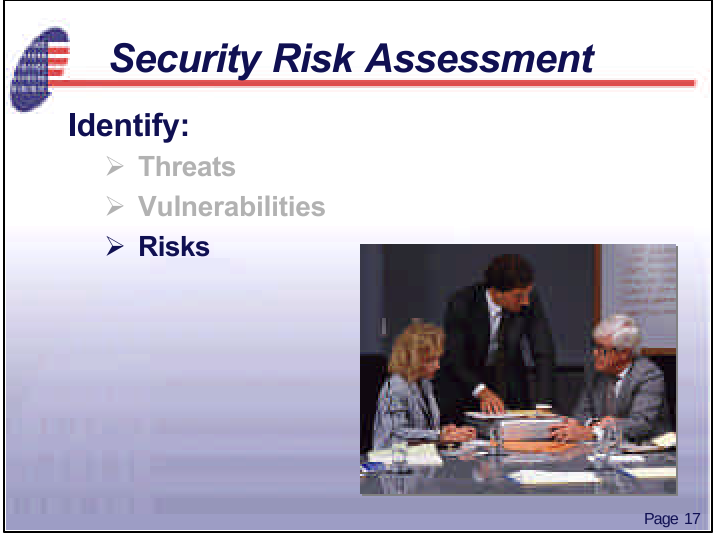
Page 16

Content Notes

You may be very vulnerable to popular attacks:
•Hacking tools are available on the internet
•]Printers may be shared
And you may have little vulnerability when attacks are less well known and harder to carry out – like a wiretap.

Presentation Notes

Give an example of each.



Security Risk Assessment

Identify:

- Threats
- Vulnerabilities
- **Risks**

Content Notes

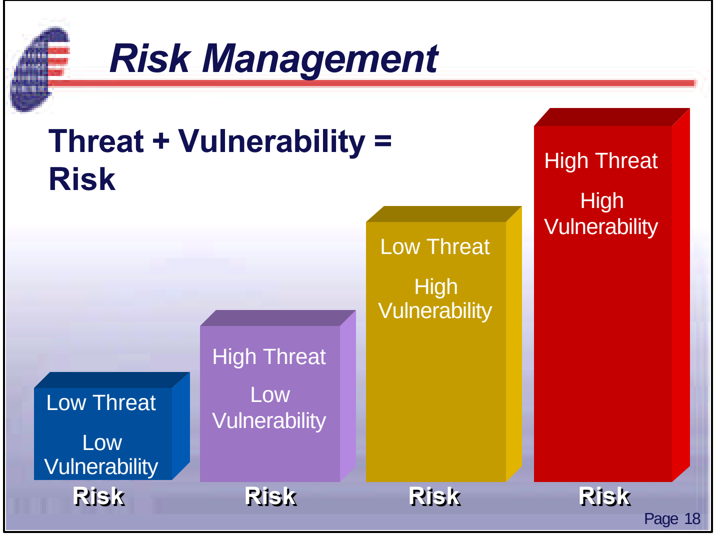
Risk is the chance that a threat will have an impact on your company.

To assess risk, ask:
•What can happen?
•How can it happen?
•What is the chance of it having an impact?

Presentation Notes

Introduce risk management

Give an example: Buying insurance for a house:
•Are you protecting yourself against a flood, a tornado?
•Where is the house located?
•What is it made of?
•How many tornados are there in an average year?



Risk Management

Threat + Vulnerability = Risk

Low Threat
Low Vulnerability
Risk

High Threat
Low Vulnerability
Risk

Low Threat
High Vulnerability
Risk

High Threat
High Vulnerability
Risk

Page 18

Content Notes

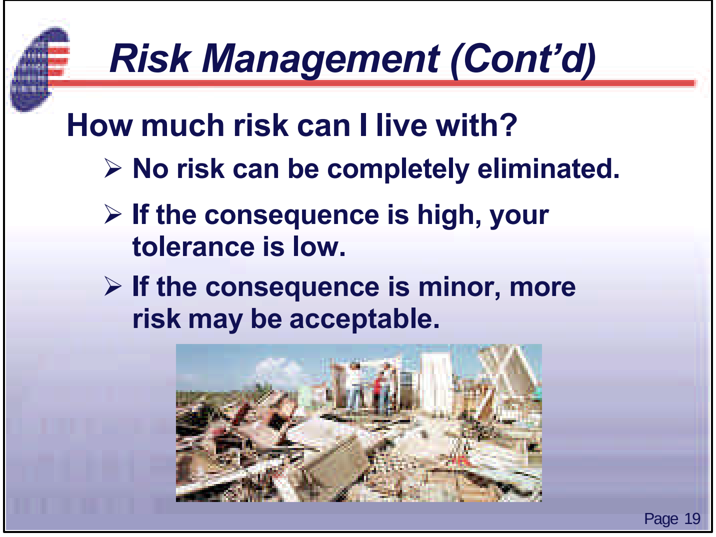
Risk is that chance that a threat will act on a vulnerability.
What is the risk that a specific threat and vulnerability will break my security?

- High Threat + High Vulnerability = High Risk
- Low Threat + Low Vulnerability = Low Risk
- Low Threat + High Vulnerability = Medium Risk
- Be careful here, this case is rare in practice
- High Threat + Low Vulnerability = Low (but non zero) Risk

Presentation Notes

Give examples as time permits.

Carry through one or more of their business examples from threat/vulnerability slides



Risk Management (Cont'd)

How much risk can I live with?

- **No risk can be completely eliminated.**
- **If the consequence is high, your tolerance is low.**
- **If the consequence is minor, more risk may be acceptable.**

Content Notes

Golden Rules of Security Risk Management:

- No risk can be completely eliminated

  Better to know the acceptable risk, than strive for total risk elimination

- The worst risks are the ones you haven't identified

  Better to know all your risks and only mitigate the ones that are important, rather than mitigate just the ones you know

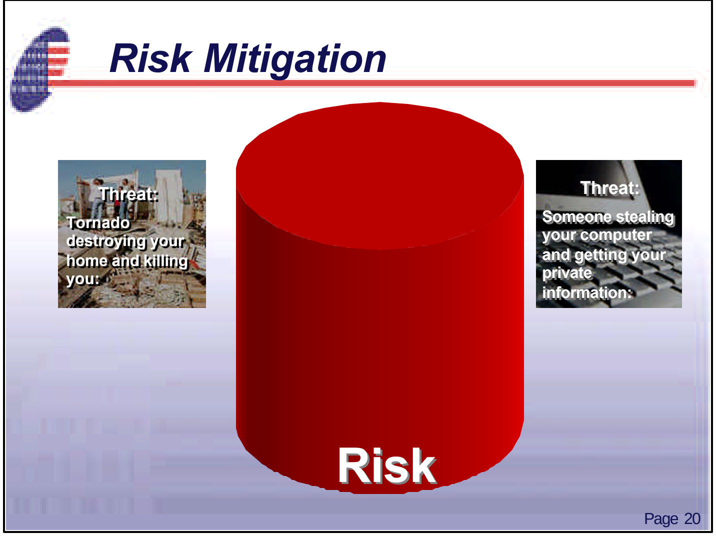
- Risk identification is an ongoing process.

How much risk can I live with?

- If the consequence to a risk is great, then very little
- If the consequence is low, then more risk may be acceptable

Presentation Notes

Point out that these are the same questions people ask themselves when considering stock investments. The answer determines the type of investment you make….



Risk Mitigation

Threat: Tornado destroying your home and killing you:

Threat: Someone stealing your computer and getting your private information:

Risk

Page 20

Content Notes

Risk Mitigation are the steps you take to reduce your security risk to an acceptable level

Can be done in three ways:

- Reduce Threat
  - Hard to do given human nature
  - Training and accountability will help with insiders
  - Scare tactics are tempting, but often temporary
- Reduce Vulnerabilities
  - Secure your enterprise and systems!
  - Use People, Processes, and Technology
- Reduce the Consequences
  - E.g. - Put no information you care about on a vulnerable computer

Presentation Notes

Use these examples:

1. Threat: Tornado destroying your home and killing you

Reducing threat: move to New England (in the notes: that's really cheating)

Reducing vulnerability: strengthen and reinforce home

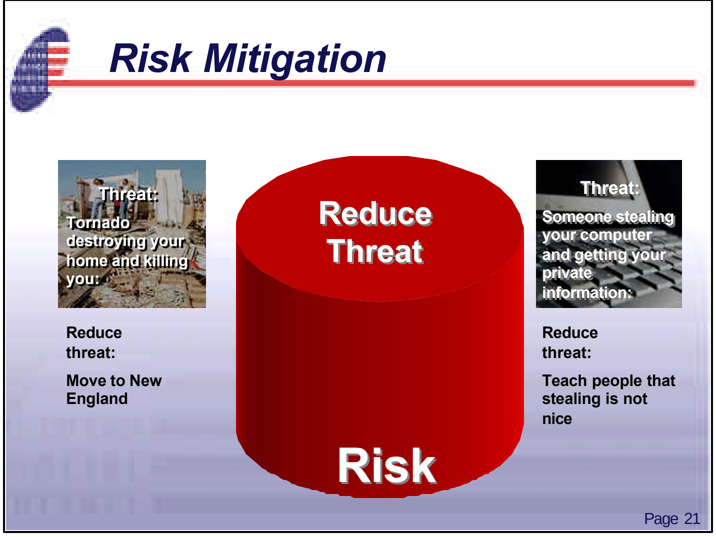
Reduce consequence: leave the home before the tornado arrives and take all your stuff with you

2. Threat: Someone stealing your computer and getting your private information

Reduce threat: Teach people that stealing is not nice

Reduce vulnerability: Keep that computer in a locked room

Reduce consequence: Put no valuable information on that computer



Risk Mitigation

Threat:
Tornado destroying your home and killing you:

Reduce threat:

Move to New England

Reduce Threat

Risk

Threat:
Someone stealing your computer and getting your private information:

Reduce threat:

Teach people that stealing is not nice

Page 21

Content Notes

Risk Mitigation are the steps you take to reduce your security risk to an acceptable level

Can be done in three ways:

- Reduce Threat
  - Hard to do given human nature
  - Training and accountability will help with insiders
  - Scare tactics are tempting, but often temporary
- Reduce Vulnerabilities
  - Secure your enterprise and systems!
  - Use People, Processes, and Technology
- Reduce the Consequences
  - E.g. - Put no information you care about on a vulnerable computer

Presentation Notes

Use these examples:

1. Threat: Tornado destroying your home and killing you

Reducing threat: move to New England (that's really cheating)

Reducing vulnerability: strengthen and reinforce home

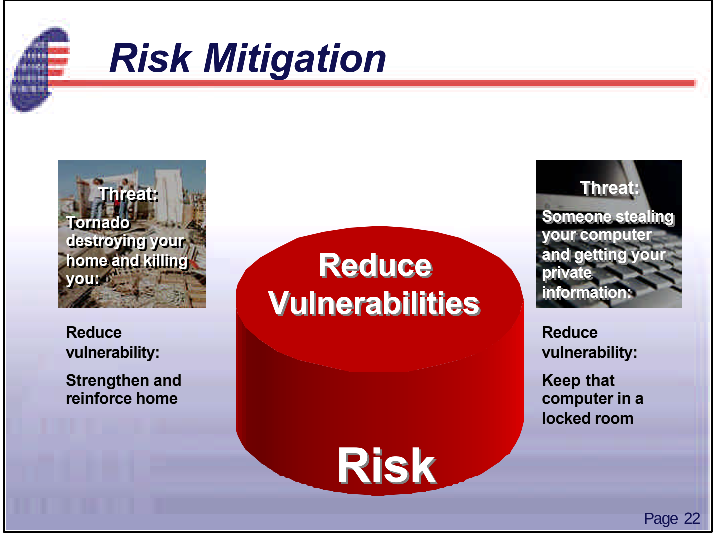
Reduce consequence: leave the home before the tornado arrives and take all your stuff with you

2. Threat: Someone stealing your computer and getting your private information

Reduce threat: Teach people that stealing is not nice

Reduce vulnerability: Keep that computer in a locked room

Reduce consequence: Put no valuable information on that computer



Risk Mitigation

Threat: Tornado destroying your home and killing you:

Reduce vulnerability:

Strengthen and reinforce home

Reduce Vulnerabilities

Risk

Threat: Someone stealing your computer and getting your private information:

Reduce vulnerability:

Keep that computer in a locked room

Page 22

Content Notes

Risk Mitigation are the steps you take to reduce your security risk to an acceptable level

Can be done in three ways:

- Reduce Threat
- Reduce Vulnerabilities
- Reduce the Consequences

Presentation Notes

Use these examples:

1. Threat: Tornado destroying your home and killing you

Reducing threat: move to New England (in the notes: that's really cheating)

Reducing vulnerability: strengthen and reinforce home

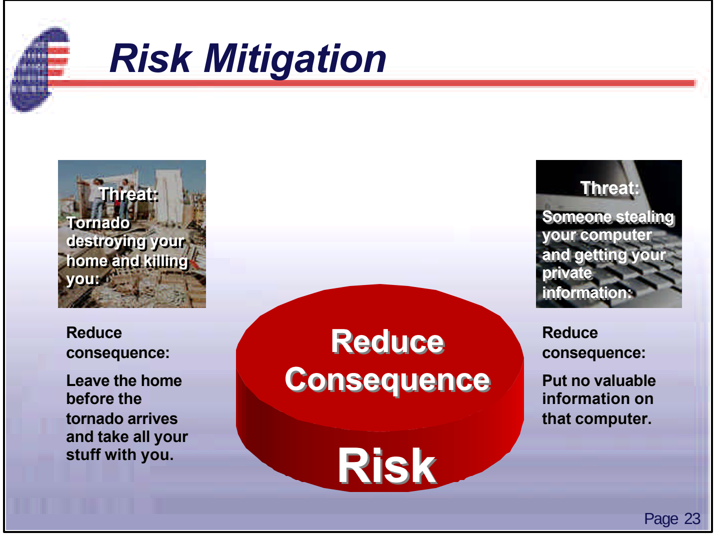
Reduce consequence: leave the home before the tornado arrives and take all your stuff with you

2. Threat: Someone stealing your computer and getting your private information

Reduce threat: Teach people that stealing is not nice

Reduce vulnerability: Keep that computer in a locked room

Reduce consequence: Put no valuable information on that computer



Risk Mitigation

Threat:
Tornado destroying your home and killing you:

Reduce consequence:

Leave the home before the tornado arrives and take all your stuff with you.

Reduce Consequence

Risk

Threat:
Someone stealing your computer and getting your private information:

Reduce consequence:

Put no valuable information on that computer.

Page 23

Content Notes

Risk Mitigation are the steps you take to reduce your security risk to an acceptable level

Presentation Notes

Use these examples:
1. Threat: Tornado destroying your home and killing you

Reducing threat: move to New England (in the notes: that's really cheating)

Reducing vulnerability: strengthen and reinforce home

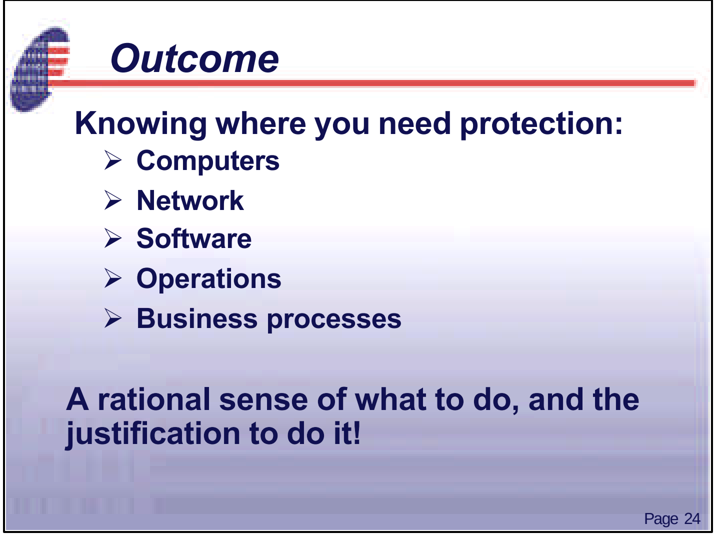
Reduce consequence: leave the home before the tornado arrives and take all your stuff with you

2. Threat: Someone stealing your computer and getting your private information

Reduce threat: Teach people that stealing is not nice

Reduce vulnerability: Keep that computer in a locked room

Reduce consequence: Put no valuable information on that computer



Outcome

Knowing where you need protection:

- Computers
- Network
- Software
- Operations
- Business processes

A rational sense of what to do, and the justification to do it!

Page 24

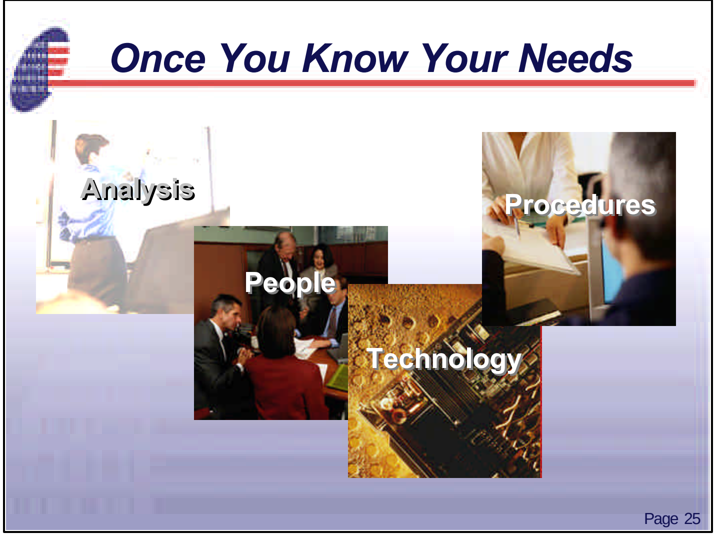
Content Notes

Risk Assessment yields Security Requirements for

- Your systems' capabilities: technology and mechanisms
- Your business applications: proper incorporation of security
- Your operational procedures: administration
- Your business process: work flow, approvals, reviews, configuration control

Know what to do and why you are doing it.

Presentation Notes



Once You Know Your Needs

Analysis

People

Procedures

Technology

Page 25

Content Notes

Now that you know what you need to protect and what potential threats and vulnerabilities you face, you can use

- People
- Procedures, and
- Technology

to provide information security.

These will be discussed in the upcoming sessions.

Presentation Notes

NOTE: Ask participants to take a few minutes to fill out the evaluation form for this presentation, which is at the end of the presentation handout. Put the filled out evaluation form on the table at the back of the room.